PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342168
(43)Date of publication of application : 29.11.2002

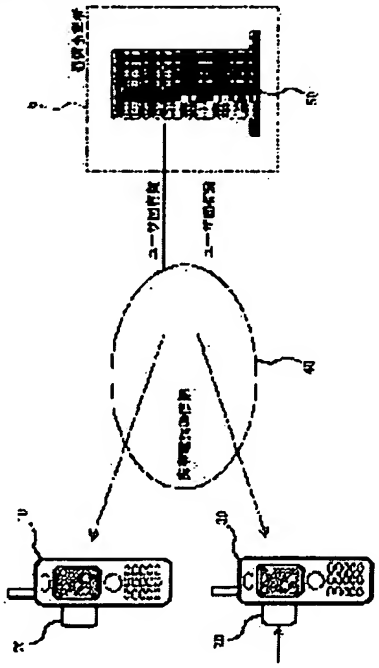
(51)Int.Cl. G06F 12/14
G06F 12/00
G09C 1/00
H04L 9/08
H04L 9/10
H04L 9/32

(21)Application number : 2001-144826
(22)Date of filing : 15.05.2001

(71)Applicant : J-PHONE EAST CO LTD
(72)Inventor : HIGUCHI KAZUHISA
UETSUKI SHINJI
FUKAYA MASATO

(54) METHOD FOR MOVING TERMINAL STORAGE DATA BETWEEN INFORMATION COMMUNICATION TERMINALS, INFORMATION PROCESSOR FOR CRYPTOGRAPHIC KEY MANAGEMENT, INFORMATION COMMUNICATION TERMINAL AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To make the movement of terminal storage data between portable telephone sets reliable while securing copyright protection to the terminal storage data stored in a portable telephone set.
SOLUTION: The terminal storage data stored in a portable telephone set 10 before exchange are enciphered by using a user-specific key downloaded from a user management server 50, the enciphered terminal storage data are written to a memory card 20, the enciphered terminal storage data written in the memory card 20 are read with an exchanged portable telephone 30, and the terminal storage data read with the exchanged portable telephone 30 are decoded by using the user-specific key downloaded from the user management server 50.



LEGAL STATUS

[Date of request for examination] 26.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－342168
（P2002－342168A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)	
G06F	12/14	320	G06F	12/14	320B	5B017
	12/00	537		12/00	537H	5B082
G09C	1/00	660	G09C	1/00	660D	5J104
H04L	9/08		H04L	9/00	601B	
	9/10				671	

審査請求　未請求　請求項の数14　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2001－144826(P2001－144826)

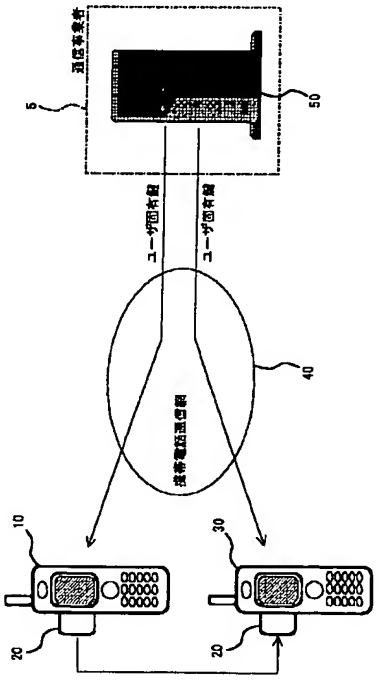
(22)出願日　平成13年５月15日(2001.5.15)

(71)出願人　594106346
ジェイフォン東日本株式会社
東京都新宿区信濃町34番地　ＪＲ信濃町ビル
(72)発明者　樋口　和久
東京都新宿区信濃町34番地　ＪＲ信濃町ビル　ジェイフォン東日本株式会社内
(72)発明者　植月　伸次
東京都新宿区信濃町34番地　ＪＲ信濃町ビル　ジェイフォン東日本株式会社内
(74)代理人　100098626
弁理士　黒田　壽

最終頁に続く

(54)【発明の名称】　情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラム

(57)【要約】
【課題】　携帯電話機に保存された端末保存データに対する著作権保護を確保しつつ、携帯電話機間の端末保存データの移動を確実に行う。
【解決手段】　ユーザ管理サーバ５０からダウンロードしたユーザ固有鍵を用いて、交換前の携帯電話機１０内に保存されている端末保存データを暗号化し、暗号化された端末保存データをメモリーカード２０に書き込み、メモリーカード２０内に暗号化して書き込んだ端末保存データを交換後の携帯電話機３０に読み込み、ユーザ管理サーバ５０からダウンロードしたユーザ固有鍵を用いて、交換後の携帯電話機３０に読み込んだ端末保存データを復号化する。



【特許請求の範囲】
【請求項１】情報通信端末に保存されている端末保存データを他の情報通信端末に移す情報通信端末間の端末保存データ移動方法であって、
利用者固有の暗号鍵情報を用いて、データ移動元の情報通信端末内に保存されている端末保存データを暗号化するステップと、
該暗号化された端末保存データを記録媒体に書き込むステップと、
該記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込むステップと、
利用者固有の暗号鍵情報を用いて、該データ移動先の情報通信端末に読み込んだ該端末保存データを復号化するステップとを実行することを特徴とする情報通信端末間の端末保存データ移動方法。
【請求項２】請求項１の情報通信端末間の端末保存データ移動方法において、
上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に着脱可能な記録媒体に書き込むことを特徴とする情報通信端末間の端末保存データ移動方法。
【請求項３】請求項１の情報通信端末間の端末保存データ移動方法において、
上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末との間で通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込むことを特徴とする情報通信端末間の端末保存データ移動方法。
【請求項４】請求項１、２又は３の情報通信端末間の端末保存データ移動方法において、
上記利用者固有の暗号鍵情報を、暗号鍵管理用情報処理装置から通信回線を介して上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に登録することを特徴とする情報通信端末間の端末保存データ移動方法。
【請求項５】情報通信端末の利用者が該情報通信端末内に保存している端末保存データを暗号化及び復号化するときに用いる利用者固有の暗号鍵情報を管理する暗号鍵管理用情報処理装置であって、
利用者固有の暗号鍵情報を生成する暗号鍵情報生成手段と、
該利用者固有の暗号鍵情報と利用者の情報とを関連づけて記憶する利用者情報記憶手段と、
該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報を、通信回線を介して該利用者の情報通信端末に送信する暗号鍵情報送信手段とを備えたことを特徴とする暗号鍵管理用情報処理装置。
【請求項６】請求項５の暗号鍵管理用情報処理装置において、
上記利用者の情報通信端末から本人確認情報を受信する本人確認情報受信手段と、該本人確認情報に基づいて、該情報通信端末を操作している利用者が本人であるかどうかを確認する本人確認手段とを備え、
上記暗号鍵情報送信手段を、該利用者が本人であることを確認したときに、上記利用者固有の暗号鍵情報を通信回線を介して該利用者の情報通信端末に送信するように構成したことを特徴とする暗号鍵管理用情報処理装置。
【請求項７】請求項５又は６の暗号鍵管理用情報処理装置に用いるコンピュータで実行するプログラムであって、
該コンピュータを、該暗号鍵管理用情報処理装置における各手段の少なくとも一つとして機能させるためのプログラム。
【請求項８】端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、
利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、
該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、
該暗号化された端末保存データを該記録媒体に書き込むデータ書込手段とを備えたことを特徴とする情報通信端末。
【請求項９】端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、
利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、
該利用者固有の暗号鍵情報を用いて、該記録媒体に記録されている暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とする情報通信端末。
【請求項１０】端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、
利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、
該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、
該暗号化された端末保存データを、通信回線を介して端末保存データ管理用情報処理装置に送信する端末保存データ送信手段とを備えたことを特徴とする情報通信端末。
【請求項１１】端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、
利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、
端末保存データ管理装置から通信回線を介して、暗号化された端末保存データを受信する端末保存データ受信手段と、
該利用者固有の暗号鍵情報を用いて、該暗号化された端

末保存データを復号化する復号化手段とを備えたことを特徴とする情報通信端末。
【請求項１２】請求項８、９、１０又は１１の情報通信端末において、
暗号鍵管理用情報処理装置から送信されてきた上記利用者固有の暗号鍵情報を、通信回線を介して受信する暗号鍵情報受信手段を備えたことを特徴とする情報通信端末。
【請求項１３】請求項１２の情報通信端末において、
通信回線を介して暗号鍵管理用情報処理装置に本人確認情報を送信する本人確認情報送信手段を備えたことを特徴とする情報通信端末。
【請求項１４】請求項８、９、１０、１１、１２又は１３の情報通信端末に用いるコンピュータで実行するプログラムであって、
該コンピュータを、上記情報通信端末における各手段の少なくとも一つとして機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報通信端末の交換等のときに、データ移動元の情報通信端末に保存されている画像データ、音楽データ、プログラムデータ等の端末保存データを、データ移動先の情報通信端末に移すための情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラムに関するものである。
【０００２】
【従来の技術】携帯電話機等の情報通信端末では、インターネット上の情報提供サイトや携帯電話通信事業者等が管理運営する情報提供システム等から、画像データ、音声データ、プログラムデータ等をダウンロードして情報通信端末内に保存し、これらのデータを情報通信端末上で表示したり起動したりして利用する場合があった。このようにインターネット等からダウンロードして情報通信端末内に保存した端末保存データの中には、著作権で保護されたものがある。特に、有料でダウンロードされた画像データ、音楽データ，ゲームなどのプログラムデータ等の多くは著作権で保護されたものである。このように著作権で保護された端末保存データは無断で複製したり第三者へ譲渡したりすることができず、基本的にデータをダウンロードした利用者の情報通信端末での使用に制限されている。
【０００３】一方、上記携帯電話機等の情報通信端末は、機種変更、故障、不具合発生等により新しい情報通信端末に交換する場合がある。この情報通信端末を交換する際に、上記インターネット等からダウンロードして交換前の情報通信端末に保存している端末保存データを、交換後の新しい情報通信端末でもそのまま使用したいときがある。
【０００４】従来、上記情報通信端末を交換するときに情報端末間で端末保存データを移す方法としては、メモリーカード等の記録媒体を用いた方法が知られている。この方法では、交換前の情報通信端末内に保存されている端末保存データを情報通信端末に装着した記録媒体に書き込み、このデータが書き込まれた記録媒体を新しい交換後の情報通信端末に装着し、記録媒体から交換後の情報通信端末内に端末保存データを読み込む。
【０００５】
【発明が解決しようとする課題】ところが、上記従来の情報通信端末間の端末保存データ移動方法では、上記メモリーカード等の記録媒体におけるデータの保護が不十分であったので、端末保存データが著作権で保護されている場合に、第三者への譲渡等を防止して著作権保護を確保しつつ、端末保存データを交換後の情報通信端末に移すことが難しかった。
【０００６】なお、上記端末保存データの著作権保護を確保するために、ユニークなID等の暗号鍵情報を用いてデータを暗号化して保存するセキュリティ機能を有するメモリーカード等の記録媒体を用いる方法が考えられる。しかしながら、この方法では、情報通信端末の利用者が端末保存データを第三者に不正に譲渡したり、他の機器に不正に複製したりすることまで防止することは難しいという問題あった。また、上記端末保存データの著作権保護を確保するために、携帯電話番号等の端末識別番号ごとに設定された端末固有の暗号鍵情報で暗号化してデータを受け渡す方法が考えられる。しかしながら、情報通信端末の交換の際に端末識別番号を変えようとすると、利用者が同じであっても交換後の情報通信端末上で暗号化された端末保存データを復号化できないという問題があった。
【０００７】本発明は以上の問題点に鑑みなされたものであり、その目的は、情報通信端末に保存された端末保存データに対する著作権保護を確保しつつ、情報通信端末間の端末保存データの移動を確実に行うことができる情報通信端末間の端末保存データ移動方法、暗号鍵管理用情報処理装置、情報通信端末及びプログラムを提供することである。
【０００８】
【課題を解決するための手段】上記目的を達成するために、請求項１の発明は、情報通信端末に保存されている端末保存データを他の情報通信端末に移す情報通信端末間の端末保存データ移動方法であって、利用者固有の暗号鍵情報を用いて、データ移動元の情報通信端末内に保存されている端末保存データを暗号化するステップと、該暗号化された端末保存データを記録媒体に書き込むステップと、該記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込むステップと、利用者固有の暗号鍵情報を用いて、該データ移動先の情報通信端末に読み込んだ該端末保存データを復号化するステップとを実行することを特徴とするもの

である。

【０００９】ここで、上記「情報通信端末」には、ＰＤＣ（Personal Digital Cellular）方式、ＧＳＭ（Global System for Mobile Communication）方式、ＴＩＡ（Telecommunications Industry Association）方式等の携帯電話機、ＩＭＴ（International Mobile Telecommunications）－２０００で標準化された携帯電話機、ＰＨＳ（Personal Handyphone Service）、自動車電話等の電話機のほか、携帯電話モジュールを付加した情報通信端末も含まれる。また、この「情報通信端末」は、上記携帯電話機などの移動型の情報通信端末でいいし、ディスクトップ型パーソナルコンピュータなどの固定型の情報通信端末であってもよい。また、上記「端末保存データ」としては、情報通信端末内に保存されている、画像データ、音楽データ、Ｊａｖａなどのプログラム言語で記述されたプログラムデータなどが挙げられる。また、上記「利用者固有の暗号鍵情報」は、情報通信端末の使用開始時にその情報通信端末内に登録してもいいし、情報通信端末での暗号化や復号化の際に外部の暗号鍵管理用情報処理装置から通信回線を介して情報通信端末に受信して登録するようにしてもよい。また、上記「利用者固有の暗号鍵情報」の生成は、情報通信端末の使用開始時に行ってもいいし、情報通信端末での暗号化や復号化の際に行ってもよい。

【００１０】請求項１の端末保存データ移動方法では、データ移動元の情報通信端末内に保存されている端末保存データを、利用者固有の暗号鍵情報を用いて暗号化して記録媒体に書き込むことにより、第三者が記録媒体からデータを読み出して復号化できないようにする。そして、上記記録媒体内に暗号化して書き込んだ端末保存データを、データ移動先の情報通信端末に読み込み、上記利用者固有の暗号化鍵情報を用いて復号化することにより、端末保存データをデータ移動先の情報通信端末で使用できるようになる。なお、上記利用者固有の暗号鍵情報はそれぞれ、データ移動元の情報通信端末内及びデータ移動先の情報通信端末内での使用に制限されているものが好ましい。この場合は、利用者固有の暗号鍵情報を他の機器に移して使用できなくなるので、利用者自身が上記記録媒体に書き込まれている端末保存データを他の機器で復号して不正に使用することを防止できる。

【００１１】請求項２の発明は、請求項１の情報通信端末間の端末保存データ移動方法において、上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に着脱可能な記録媒体に書き込むことを特徴とするものである。ここで、上記「着脱可能な記録媒体」には、ＳＤメモリーカードのほか、ＣＦ（コンパクトフラッシュ（登録商標））メモリーカード、スマートメディア、メモリースティック、ＭＭＣ（マルチメディアカード）等も含まれる。

【００１２】請求項２の端末保存データ移動方法では、データ移動元の情報通信端末に装着した記録媒体に上記暗号化された端末保存データを書き込む。そして、この記録媒体をデータ移動先の情報通信端末に装着することにより、記録媒体内の暗号化された端末保存データを読み込んで復号化し、データ移動先の情報通信端末で使用できる。

【００１３】請求項３の発明は、請求項１の情報通信端末間の端末保存データ移動方法において、上記暗号化された端末保存データを、上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末との間で通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込むことを特徴とするものである。

【００１４】請求項３の端末保存データ移動方法では、データ移動元の情報通信端末内の暗号化された端末保存データを、通信回線を介してデータの送受信可能な情報処理装置内の記録媒体に書き込む。そして、この情報処理装置から送信された暗号化済みの端末保存データをデータ移動先の情報通信端末で受信して復号化し、データ移動先の情報通信端末で使用できる。

【００１５】請求項４の発明は、請求項１、２又は３の情報通信端末間の端末保存データ移動方法において、上記利用者固有の暗号鍵情報を、暗号鍵管理用情報処理装置から通信回線を介して上記データ移動元の情報通信端末及び上記データ移動先の情報通信端末に登録することを特徴とするものである。

【００１６】請求項４の端末保存データ移動方法では、上記利用者固有の暗号鍵情報が、通信回線を介して暗号鍵管理用情報処理装置から登録できるため、各利用者の情報通信端末で用いる利用者固有の暗号鍵情報を一元管理できるようになる。

【００１７】請求項５の発明は、情報通信端末の利用者が該情報通信端末内に保存している端末保存データを暗号化及び復号化するときに用いる利用者固有の暗号鍵情報を管理する暗号鍵管理用情報処理装置であって、利用者固有の暗号鍵情報を生成する暗号鍵情報生成手段と、該利用者固有の暗号鍵情報と利用者の情報とを関連づけて記憶する利用者情報記憶手段と、該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報を、通信回線を介して該利用者の情報通信端末に送信する暗号鍵情報送信手段とを備えたことを特徴とするものである。

【００１８】請求項５の暗号鍵管理用情報処理装置では、暗号鍵情報生成手段で利用者固有の暗号鍵情報が生成され、利用者固有の暗号鍵情報と利用者の情報と関連づけられて利用者情報記憶手段に記憶される。そして、暗号鍵情報送信手段により、該利用者情報記憶手段に記憶されている利用者固有の暗号鍵情報が、通信回線を介して該利用者の情報通信端末に送信される。暗号鍵管理用情報処理装置から送信された利用者固有の暗号鍵情報は、各利用者の情報通信端末で受信されて登録され、端

末保存データの暗号化及び復号化に用いられる。

【００１９】請求項６の発明は、請求項５の暗号鍵管理用情報処理装置において、上記利用者の情報通信端末から本人確認情報を受信する本人確認情報受信手段と、該本人確認情報に基づいて、該情報通信端末を操作している利用者が本人であるかどうかを確認する本人確認手段とを備え、上記暗号鍵情報送信手段を、該利用者が本人であることを確認したときに、上記利用者固有の暗号鍵情報を通信回線を介して該利用者の情報通信端末に送信するように構成したことを特徴とするものである。

【００２０】請求項６の暗号鍵管理用情報処理装置では、本人確認情報受信手段で利用者の情報通信端末から本人確認情報が受信され、この本人確認情報に基づいて、本人確認手段により該情報通信端末を操作している利用者が本人であるかどうかが確認される。そして、上記暗号鍵取得要求データを送ってきた利用者が本人であると確認されたときに、上記暗号鍵情報送信手段により、利用者固有の暗号鍵情報が通信回線を介して利用者の情報通信端末に送信される。

【００２１】請求項７の発明は、請求項５又は６の暗号鍵管理用情報処理装置に用いるコンピュータで実行するプログラムであって、該コンピュータを、該暗号鍵管理用情報処理装置における各手段の少なくとも一つとして機能させるためのプログラムである。

【００２２】請求項７のプログラムを暗号鍵管理用情報処理装置で用いるコンピュータで実行することにより、暗号鍵管理用情報処理装置における各種情報処理を実行することができる。

【００２３】請求項８の発明は、端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、該暗号化された端末保存データを該記録媒体に書き込むデータ書込手段とを備えたことを特徴とするものである。

【００２４】請求項８の情報通信端末では、端末保存データ記憶手段に記憶されている端末保存データが利用者固有の暗号鍵情報を用いて暗号化されて記録媒体に書き込まれるため、第三者が記録媒体からデータを読み出して復号化できない。

【００２５】請求項９の発明は、端末保存データを記憶する端末保存データ記憶手段を備え、記録媒体が着脱可能な情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該記録媒体に記録されている暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とするものである。

【００２６】請求項９の情報通信端末では、記録媒体内の暗号化された端末保存データが読み出され、利用者固有の暗号鍵情報を用いて復号化されて使用可能となる。

【００２７】請求項１０の発明は、端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、該利用者固有の暗号鍵情報を用いて、該端末保存データを暗号化する暗号化手段と、該暗号化された端末保存データを、通信回線を介して端末保存データ管理用情報処理装置に送信する端末保存データ送信手段とを備えたことを特徴とするものである。

【００２８】請求項１０の情報通信端末では、端末保存データ記憶手段に記憶されている端末保存データが利用者固有の暗号鍵情報を用いて暗号化され、通信回線を介して端末保存データ管理用情報処理装置に送信されて管理されるため、第三者がデータを読み出して復号化できない。

【００２９】請求項１１の発明は、端末保存データを記憶する端末保存データ記憶手段を備えた情報通信端末であって、利用者固有の暗号鍵情報を記憶する暗号鍵情報記憶手段と、端末保存データ管理装置から通信回線を介して、暗号化された端末保存データを受信する端末保存データ受信手段と、該利用者固有の暗号鍵情報を用いて、該暗号化された端末保存データを復号化する復号化手段とを備えたことを特徴とするものである。

【００３０】請求項１１の情報通信端末では、暗号化された端末保存データが端末保存データ管理装置から通信回線を介して受信され、利用者固有の暗号鍵情報を用いて復号化されて使用可能となる。

【００３１】なお、上記請求項８、９、１０及び１１の情報通信端末で用いる利用者固有の暗号鍵情報はそれぞれ、情報通信端末内での使用に制限された状態で上記暗号化鍵情報記憶手段に記憶するのが好ましい。この場合は、利用者固有の暗号鍵情報を他の機器に移して使用できなくなるので、利用者自身が上記暗号化されている端末保存データを他の機器で復号して不正に使用することを防止できる。

【００３２】請求項１２の発明は、請求項８、９、１０又は１１の情報通信端末において、暗号鍵管理用情報処理装置から送信されてきた上記利用者固有の暗号鍵情報を、通信回線を介して受信する暗号鍵情報受信手段を備えたことを特徴とするものである。

【００３３】請求項１２の情報通信端末では、必要に応じて、暗号鍵管理用情報処理装置から送信されてきた利用者固有の暗号鍵情報を、通信回線を介して受信し、端末保存データの暗号化や復号化に用いることができる。

【００３４】請求項１３の発明は、請求項１２の情報通信端末において、通信回線を介して暗号鍵管理用情報処理装置に本人確認情報を送信する本人確認情報送信手段を備えたことを特徴とするものである。

【００３５】請求項１３の情報通信端末では、本人確認情報送信手段で通信回線を介して暗号鍵管理用情報処理

装置に本人確認情報を送信することにより、暗号鍵管理用情報処理装置で利用者の本人確認を行った後、利用者固有の暗号鍵情報を情報通信端末に送信することができるようになる。

【００３６】請求項１４の発明は、請求項８、９、１０、１１、１２又は１３の情報通信端末に用いるコンピュータで実行するプログラムであって、該コンピュータを、上記情報通信端末における各手段の少なくとも一つとして機能させるためのプログラムである。

【００３７】請求項１４のプログラムを情報処理端末で用いるコンピュータで実行することにより、情報通信端末における各種情報処理を実行することができる。

【００３８】なお、上記請求項７又は１４の発明に係るプログラムの受け渡しは、デジタル情報としてプログラムを記録したＦＤ，ＣＤ－ＲＯＭ等の記録媒体を用いて行なってもいいし、コンピュータネットワーク等の通信回線を用いて行なってもよい。

【００３９】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。

〔実施形態１〕図１は、本発明の第１の実施形態に係る端末保存データ移動方法の概念図である。本実施形態の端末保存データ移動方法は、情報通信端末としての携帯電話機を機種変更等の理由で交換するときに、データ移動元の携帯電話機（以下「交換前の携帯電話機」という。）からデータ移動先の新しい携帯電話機（以下「交換後の携帯電話機」という。）に、有料でダウンロードした待ち受け画面等の画像データ、着信メロディ等の音楽データ、ゲームソフトなどのＪａｖａプログラムデータなどの著作権で保護されている端末保存データを移す方法である。

【００４０】図１において、交換前の携帯電話機１０内に保存されている端末保存データは、交換前の携帯電話機１０内での使用に制限されている利用者固有の暗号鍵情報（以下、「ユーザ固有鍵」という。）を用いて暗号化され、携帯電話機１０に着脱可能な記録媒体としてのメモリーカード２０に書き込まれる。上記メモリーカード２０は交換後の携帯電話機３０に装着され、メモリーカード２０内に暗号化して書き込まれた端末保存データが、交換後の携帯電話機３０に読み込まれる。交換後の携帯電話機３０は、交換後の携帯電話機３０での使用に制限されているユーザ固有鍵を用いて復号化される。上記交換前後の携帯電話機１０、３０で使用されるユーザ固有鍵は、通信回線としての携帯電話通信網４０を介して、通信事業者５が管理運営する暗号鍵管理用情報処理装置としてのユーザ管理サーバ５０からダウンロードされる。

【００４１】図２及び図３はそれぞれ、本端末保存データ移動方法に用いられるユーザ管理サーバ５０の概略構成図及び機能ブロック図である。このユーザ管理サーバ５０は通信事業者５によって管理運営され、図２に示すように、システムバス１００、ＣＰＵ１０１、ＲＡＭ１０２やＲＯＭ１０３等からなる内部記憶装置、ハードディスクドライブ（ＨＤＤ）や光ディスクドライブ等からなる外部記憶装置１０４、マウスやキーボード等からなる入力装置１０５、ディスプレイやプリンタ等からなる出力装置１０６、及び携帯電話通信網４０を介して各利用者１０の携帯電話機６０と通信するための携帯電話用通信装置１０８を備えている。ＣＰＵ１０１やＲＡＭ１０２等の構成要素はお互いに、システムバス１００を介して、データやプログラムの命令等のやり取りを行っている。この認証システム５１を所定の手順に従って動作させるためのプログラムはＲＯＭ１０３や外部記憶装置１０４に記憶されており、必要に応じてＣＰＵ１０１やＲＡＭ１０２上の作業エリアに呼び出されて実行される。また、上記ユーザ管理サーバ５０は１台のコンピュータシステムで構成してもいいし、各種データを関連付けて管理するデータベースサーバ等のような複数のサーバ機能をそれぞれ受け持つ複数台のコンピュータをネットワークで結んで構成してもよい。

【００４２】ユーザ管理サーバ５０は、図２に示したハードウェア上で所定のプログラムを実行することにより、図３に示す利用者情報記憶手段５０１、暗号鍵情報生成手段５０２及び暗号鍵情報送信手段５０３の各機能を実現している。上記利用者情報記憶手段５０１は、上記ユーザ管理サーバ５０のハードディスク等からなる外部記憶装置１０４を用いて構成されており、携帯電話機１０，３０を所有している利用者に関する利用者情報と、ユーザ固有鍵とを関連付けて記憶している。この利用者情報は、各利用者について、端末識別情報としての携帯電話番号や、本人確認情報としてのＰＩＮコード等が関連付けられて登録されている。

【００４３】また、上記ユーザ固有鍵としては、様々な暗号アルゴリズムで使用する暗号鍵を使用することができ、鍵長についても特定の鍵長に制限されるものではない。また、上記ユーザ鍵は、暗号化する側と復号化する側で同じものを使用する共有型の暗号鍵でもいいし、公開鍵と秘密鍵との組み合わせのように暗号化する側と復号化する側で異なるものを使用する暗号鍵であってもよい。

【００４４】上記暗号鍵情報生成手段５０２は、上記ユーザ管理サーバ５０のＣＰＵ１０１、ＲＡＭ１０２等により構成され、各利用者ごとに異なるユーザ固有鍵を生成する機能を有している。

【００４５】上記暗号鍵情報送信手段５０３は、上記ユーザ管理サーバ５０のＣＰＵ１０１、ＲＡＭ１０２、携帯電話用通信装置１０８等により構成され、利用者情報記憶手段５０１に記憶されているユーザ固有鍵を、携帯電話通信網４０を介して各利用者の携帯電話機１０、３０に送信する機能を有している。

【００４６】図４及び図５はそれぞれ、本端末保存データ移動方法に用いられる携帯電話機１０、３０の概略構成図及び機能ブロック図である。この携帯電話機１０、３０は、図４に示すように、システムバス２００、ＣＰＵ２０１、ＲＡＭ２０２やＲＯＭ２０３等からなる内部記憶装置、マイクや各種入力ボタン等からなる入力装置２０４、液晶ディスプレイ（ＬＣＤ）やスピーカ等からなる出力装置２０５、メモリーカードに対するデータ書込及びデータ読出を行うメモリーカードドライブ装置２０６、携帯電話通信網４０を介して他の携帯電話機や上記ユーザ管理サーバ５０と通信するための携帯電話用通信装置２０７を備えている。ＣＰＵ２０１やＲＡＭ２０２等の構成要素はお互いに、システムバス２００を介して、データやプログラムの命令等のやり取りを行っている。この携帯電話機１０、３０を所定の手順に従って動作させるためのプログラムはＲＯＭ２０３に記憶されており、必要に応じてＣＰＵ２０１やＲＡＭ２０２上の作業エリアに呼び出されて実行される。

【００４７】上記メモリーカード２０としては例えばＳＤメモリーカードを使用することができる。また、このＳＤメモリーカード以外にも、ＣＦ（コンパクトフラッシュ）メモリーカード、スマートメディア、メモリースティック、ＭＭＣ（マルチメディアカード）等を使用することができる。

【００４８】本携帯電話機１０、３０は、図４に示したハードウェア上で所定のプログラムを実行することにより、図５に示す端末保存データ記憶手段６０１、暗号鍵情報受信手段６０２、暗号鍵情報記憶手段６０３、暗号化手段６０４、データ書込手段６０５、データ読込手段６０６及び復号化手段６０７の各機能を実現している。

【００４９】上記端末保存データ記憶手段６０１は、携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２等により構成され、インターネット上の情報提供サイトや携帯電話通信事業者等が管理運営する情報提供システム等から待ち受け画面等の画像データ、着信メロディ等の音楽データ、ゲームソフトなどのＪａｖａプログラムデータなどの端末保存データを記憶している。

【００５０】上記暗号鍵情報受信手段６０２は、携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２、携帯電話通信網用通信装置２０７等により構成され、上記ユーザ管理サーバ５０から携帯電話通信網４０を介してユーザ固有鍵を受信する機能を有している。

【００５１】上記暗号鍵情報記憶手段６０３は、携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２等により構成され、上記暗号鍵情報受信手段６０２で受信したユーザ固有鍵を、携帯電話機内で使用に限定した状態で記憶する機能を有している。

【００５２】上記暗号化手段６０４は、携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２等により構成され、上記暗号鍵情報記憶手段６０３に記憶されているユーザ固有鍵を用いて、上記端末保存データ記憶手段６０１に記憶されている端末保存データを所定の暗号アルゴリズムにより暗号化する機能を有している。

【００５３】上記データ書込手段６０５は、携帯電話機１０、３０のＣＰＵ２０１、メモリーカードドライブ装置２０６等により構成され、上記暗号化手段６０４で暗号化された端末保存データを、携帯電話機に装着されたメモリーカード２０に書き込む機能を有している。

【００５４】上記データ読込手段６０６は、携帯電話機１０、３０のＣＰＵ２０１、メモリーカードドライブ装置２０６等により構成され、携帯電話機に装着されたメモリーカード２０内に保存されている暗号化済みの端末保存データを、携帯電話機１０、３０内に読み込む機能を有している。

【００５５】上記復号化手段６０７は、携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２等により構成され、上記暗号鍵情報記憶手段６０３に記憶されているユーザ固有鍵を用いて、上記データ読込手段６０６でメモリーカード２０から読み込んだ暗号化済みの端末保存データを所定のアルゴリズムで復号化する機能を有している。復号化された端末保存データは、上記端末保存データ記憶手段６０１に記憶され、利用者の操作により液晶ディスプレイ（ＬＣＤ）上に表示したりスピーカから出力したりすることができる。

【００５６】図６は、本実施形態の端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャートである。図６中の細い実線で囲まれたステップは交換前の携帯電話機１０での処理であり、太い実線で囲まれたステップはユーザ管理サーバ５０での処理である。また、図６中の破線で囲まれたステップは、交換後の携帯電話機３０での処理である。

【００５７】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機１０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ１）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、交換前の携帯電話機１０の利用者に対するユーザ固有鍵が生成され、携帯電話通信網４０を介して交換前の携帯電話機１０に送信される（ステップ２）。上記ユーザ固有鍵を受信した交換前の携帯電話機１０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ３）。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、交換前の携帯電話機１０に装着したメモリーカード２０に書き込まれる（ステップ４、５）。次に、交換前の携帯電話機１０からメモリーカード２０が取り外された後、交換後の新しい携帯電話機３０に装着され、メモリーカード２０内の暗号化済みの端末保存データが交換後の携帯電話機３０に読み込みこまれる（ステップ６）。そして、このデータ読み込みとともに、ユーザ固有鍵をダウンロードするためのユ

ーザ固有鍵要求データが、交換後の携帯電話機３０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ７）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、上記交換前の携帯電話機１０に対して送信したものと同じユーザ固有鍵が、携帯電話通信網４０を介して交換後の携帯電話機３０に送信される（ステップ８）。上記ユーザ管理サーバ５０から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機３０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ９）。そして、上記メモリーカード２０から読み込まれた暗号化済みの端末保存データが、暗号鍵情報記憶手段６０３に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段６０１に保存され、利用者が使用できる状態になる（ステップ１０）。

【００５８】図７は、本実施形態の端末保存データ移動方法における他のデータ移動手順の流れを示すフローチャートである。上記図６の場合と同様に、図７中の細い実線で囲まれたステップは交換前の携帯電話機１０での処理であり、太い実線で囲まれたステップはユーザ管理サーバ５０での処理である。また、図７中の破線で囲まれたステップは、交換後の携帯電話機３０での処理である。

【００５９】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機１０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ１）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、交換前の携帯電話機１０の利用者に対するユーザ固有鍵が生成され、携帯電話通信網４０を介して交換前の携帯電話機１０に送信される（ステップ２）。上記ユーザ固有鍵を受信した交換前の携帯電話機１０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ３）。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、交換前の携帯電話機１０に装着したメモリーカード２０に書き込まれる（ステップ４、５）。次に、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換後の携帯電話機３０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ６）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、上記交換前の携帯電話機１０に対して送信したものと同じユーザ固有鍵が、携帯電話通信網４０を介して交換後の携帯電話機３０に送信される（ステップ７）。そして、上記ユーザ管理サーバ５０から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機３０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ８）。次に、交換前の携帯電話機１０からメモリーカード２０が取り外された後、交換後の新しい携帯電話機３０に装着され、メモリーカード２０内の暗号化済みの端末保存データが交換後の携帯電話機３０に読み込みこまれる（ステップ９）。そして、このメモリーカード２０から読み込まれた暗号化済みの端末保存データが、暗号鍵情報記憶手段６０３に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段６０１に保存され、利用者が使用できる状態になる（ステップ１０）。

【００６０】なお、上記図６及び図７の例では、ユーザ管理サーバ５０においてユーザの携帯電話機１０からユーザ固有鍵要求データを受信したタイミングでユーザ固有鍵を生成しているが、ユーザ固有鍵は、各ユーザの携帯電話機にダウンロードして利用できる任意のタイミングで生成することができる。例えば、ユーザによる携帯電話機の使用開始にあたって利用者情報をユーザ管理サーバ５０に登録する際に、ユーザ管理サーバ５０内でそのユーザに対応するユーザ固有鍵を予め生成して記憶しておくようにしてもよい。この場合は、ユーザ固有鍵要求データを送信してからユーザ固有鍵をダウンロードするまでの時間が短くなるので、データ移動作業の効率化を図ることができる。

【００６１】以上、本実施形態によれば、携帯電話機１０、３０内での使用に制限されているユーザ固有鍵を用いて暗号化し、端末保存データを携帯電話機１０、３０間で移動させることができる。従って、携帯電話機に保存された端末保存データが、有料サイトなどからダウンロードした画像データ、音楽データ、Ｊａｖａプログラムデータ等の著作権で保護されている場合であっても、これらの端末保存データに対する著作権保護を確保しつつ、携帯電話機の交換時における端末保存データの移動を確実に行うことができる。

【００６２】〔実施形態２〕図８は、本発明の第２の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図である。以下、前述の第１の実施形態の端末保存データ移動方法と同様な部分については、同じ符号を付して説明を省略する。本実施形態の端末保存データ移動方法では、交換前の携帯電話機１０で暗号化した端末保存データをメモリーカードに書き込む代わりに、携帯電話通信網４０を介してユーザ管理サーバ５０に送信して保存し、交換後の携帯電話機３０では、携帯電話通信網４０を介してユーザ管理サーバ５０から暗号化済みの端末保存データを読み込んでいる。

【００６３】図９は、本端末保存データ移動方法に用いられるユーザ管理サーバ５０の機能ブロック図である。なお、このユーザ管理サーバ５０のハードウェア構成としては、上記第１の実施形態で示した図２の構成と同様なものを用いることができる。本ユーザ管理サーバ５０は、図２に示したハードウェア上で所定のプログラムを実行することにより、第１の実施形態における利用者情報記憶手段５０１、暗号鍵情報生成手段５０２及び暗号鍵情報送信手段５０３の各機能のほか、端末保存データ

受信手段５０４、端末保存データ記憶手段５０５及び端末保存データ送信手段５０６の各機能を実現している。

【００６４】上記端末保存データ受信手段５０４は、上記ユーザ管理サーバ５０のＣＰＵ１０１、ＲＡＭ１０２、携帯電話用通信装置１０８等により構成され、交換前の携帯電話機１０から携帯電話通信網４０を介して送信されてきた暗号化済みの端末保存データを受信する機能を有している。上記端末保存データ記憶手段５０５は、上記ユーザ管理サーバ５０のＣＰＵ１０１、ＲＡＭ１０２等により構成され、交換前の携帯電話機１０から受信した暗号化済みの端末保存データを記憶する機能を有している。上記端末保存データ送信手段５０６は、上記ユーザ管理サーバ５０のＣＰＵ１０１、ＲＡＭ１０２、携帯電話用通信装置１０８等により構成され、交換後の携帯電話機３０からのダウンロード要求に基づいて、携帯電話通信網４０を介して交換後の携帯電話機３０に暗号化済みの端末保存データを送信する機能を有している。

【００６５】図１０は、本端末保存データ移動方法に用いられる携帯電話機１０、３０の機能ブロック図である。なお、この携帯電話機１０、３０のハードウェア構成としては、メモリーカードドライブ装置２０６が必須でない点を除いて、上記第１の実施形態で示した図４の構成と同様なものを用いることができる。本携帯電話機１０、３０は、図４に示したハードウェア上で所定のプログラムを実行することにより、第１の実施形態における端末保存データ記憶手段６０１、暗号鍵情報受信手段６０２、暗号鍵情報記憶手段６０３、暗号化手段６０４及び復号化手段６０７のほか、端末保存データ送信手段６０８及び端末保存データ受信手段６０９の各機能を実現している。

【００６６】上記端末保存データ送信手段６０８は、上記携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２、携帯電話通信網用通信装置２０７等により構成され、携帯電話通信網４０を介して上記ユーザ管理サーバ５０に暗号化済みの端末保存データを送信する機能を有している。上記端末保存データ受信手段６０９は、上記携帯電話機１０、３０のＣＰＵ２０１、ＲＡＭ２０２、携帯電話通信網用通信装置２０７等により構成され、上記ユーザ管理サーバ５０から携帯電話通信網４０を介して送信されてきた暗号化済みの端末保存データを受信する機能を有している。

【００６７】図１１は、本実施形態の端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャートである。上記図６及び図７の場合と同様に、図１１中の細い実線で囲まれたステップは交換前の携帯電話機１０での処理であり、太い実線で囲まれたステップはユーザ管理サーバ５０での処理である。また、図１１中の破線で囲まれたステップは、交換後の携帯電話機３０での処理である。

【００６８】まず、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換前の携帯電話機１０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ１）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、交換前の携帯電話機１０の利用者に対するユーザ固有鍵が生成され、携帯電話通信網４０を介して交換前の携帯電話機１０に送信される（ステップ２）。上記ユーザ固有鍵を受信した交換前の携帯電話機１０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ３）。そして、このユーザ固有鍵を用いて移動対象の端末保存データが暗号化され、携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ４、５）。次に、ユーザ管理サーバ５０では、交換前の携帯電話機１０から送信されてきた暗号化済みの端末保存データが受信され、端末保存データ記憶手段５０５に保存される（ステップ６）。そして、交換後の携帯電話機３０からユーザ管理サーバ５０に端末保存データ要求データが送信されると（ステップ７）、ユーザ管理サーバ５０では、その利用者に対応した暗号化済みの端末保存データが携帯電話通信網４０を介して交換後の携帯電話機３０に送信される（ステップ８）。次に、交換後の新しい携帯電話機３０では、上記ユーザ管理サーバ５０から送信されてきた暗号化済みの端末保存データを受信し（ステップ９）、この受信とともに、ユーザ固有鍵をダウンロードするためのユーザ固有鍵要求データが、交換後の携帯電話機３０から携帯電話通信網４０を介してユーザ管理サーバ５０に送信される（ステップ１０）。ユーザ固有鍵要求データを受信したユーザ管理サーバ５０では、上記交換前の携帯電話機１０に対して送信したものと同じユーザ固有鍵が、携帯電話通信網４０を介して交換後の携帯電話機３０に送信される（ステップ１１）。上記ユーザ管理サーバ５０から送信されてきたユーザ固有鍵を受信した交換後の携帯電話機３０では、受信したユーザ固有鍵が暗号鍵情報記憶手段６０３に一旦保存される（ステップ１２）。そして、上記ユーザ管理サーバ５０から受信した暗号化済みの端末保存データが、暗号鍵情報記憶手段６０３に記憶されているユーザ固有鍵を用いて復号化され、所定の端末保存データ記憶手段６０１に保存され、利用者が使用できる状態になる（ステップ１３）。

【００６９】なお、上記図１１の例においても、前述の図６及び図７の場合と同様に、ユーザ管理サーバ５０においてユーザの携帯電話機１０からユーザ固有鍵要求データを受信したタイミングでユーザ固有鍵を生成しているが、ユーザ固有鍵は、各ユーザの携帯電話機にダウンロードして利用できる任意のタイミングで生成することができる。例えば、ユーザによる携帯電話機の使用開始にあたって利用者情報をユーザ管理サーバ５０に登録する際に、ユーザ管理サーバ５０内でそのユーザに対応す

るユーザ固有鍵を予め生成して記憶しておくようにしてもよい。この場合は、ユーザ固有鍵要求データを送信してからユーザ固有鍵をダウンロードするまでの時間が短くなるので、データ移動作業の効率化を図ることができる。

【００７０】以上、本実施形態においても、携帯電話機１０、３０内での使用に制限されているユーザ固有鍵を用いて暗号化し、端末保存データを携帯電話機１０、３０間で移動させることができる。従って、携帯電話機に保存された端末保存データが、有料サイトなどからダウンロードした画像データ、音楽データ、Ｊａｖａプログラムデータ等の著作権で保護されている場合であっても、これらの端末保存データに対する著作権保護を確保しつつ、携帯電話機の交換時における端末保存データの移動を確実に行うことができる。特に、本実施形態では、交換前後の携帯電話機の少なくとも一方がメモリーカードを使用できない場合でも、端末保存データを確実に移動させることができる。

【００７１】なお、上記第２の実施形態では、ユーザ固有鍵を管理する機能と携帯電話機から送られてきた暗号化済みの端末保存データを管理する機能を、１台のユーザ管理サーバ５０に持たせるようにしているが、各機能を別々のサーバで実現するように構成してもよい。また、上記第２の実施形態では、交換後の携帯電話機３０において、暗号化済みの端末保存データをダウンロードした後、ユーザ固有鍵をダウンロードしているが、各ダウンロードのタイミングはこれに限定されるものではなく、例えば、暗号化済みの端末保存データに先立ってユーザ固有鍵を予めダウンロードしておいてもよい。

【００７２】また、上記各実施形態において、利用者の携帯電話機１０、３０からユーザ管理サーバ５０にユーザ固有鍵要求データを送信するときに、セキュリティを高めるために、本人確認情報としてのＰＩＮ（Personl Identification Number）コードも送信し、ユーザ管理サーバ５０側で本人確認を行なった後、その利用者に対応したユーザ固有鍵を携帯電話機１０、３０に送信するようにしてもよい。この本人確認情報としては、上記ＰＩＮコードのほか、利用者の指紋情報、眼球の虹彩情報や網膜情報、手等の表面から読みとった血管情報、顔の形、音声の特徴や声紋、手形や掌紋等のバイオメトリクス（生物学的な特徴）に関する情報を用いることができる。また、文字の書き方や筆圧、筆を離す方向などの情報や、キーボードなどから入力するときのスピード等の筆跡情報や、キーと別なキーとを押す間の間隔等の打鍵情報などを用いてもよい。

【００７３】また、上記各実施形態では、ユーザ固有鍵をユーザ管理サーバ５０からダウンロードして携帯電話機内での暗号化や復号化に使用しているが、利用者による携帯電話機の使用開始時に、携帯電話機内に搭載されているメモリーに保存するようにしてよい。この場合、セキュリティを高めて著作権保護を確保するために、指紋モジュールや、次世代移動通信システム用のＳＩＭカードであるＵＳＩＭ（Universal Subscriber Identity Module）のようなセキュアメモリーに、ユーザ固有鍵を保存するのが好ましい。

【００７４】また、上記各実施形態では、情報通信端末が携帯電話機の場合について説明したが、本発明は、ＰＨＳ、自動車電話、携帯型のパソコンなどの他の移動情報端末のほか、固定型のディスクトップパソコンの場合についても適用でき、同様な効果が得られるものである。

【００７５】

【発明の効果】請求項１乃至１４の発明によれば、利用者固有の暗号鍵情報を用いて暗号化し、端末保存データを情報通信端末間で移動させることができるので、情報通信端末に保存された端末保存データが著作権で保護されている場合であっても、端末保存データに対する著作権保護を確保しつつ、情報通信端末間の端末保存データの移動を確実に行うことができるという優れた効果がある。

【００７６】特に、請求項２の発明によれば、情報通信端末に着脱可能な記録媒体を用いることにより、情報通信端末間の端末保存データの移動が簡易になるという優れた効果がある。

【００７７】特に、請求項３の発明によれば、情報通信端末が端末保存データ移動のための記録媒体を装着できる機能を有しない場合でも、情報通信端末間の端末保存データの移動が可能になるという優れた効果がある。

【００７８】特に、請求項４の発明によれば、各利用者の情報通信端末で用いる利用者固有の暗号鍵情報を一元管理できるようになるという優れた効果がある。

【００７９】特に、請求項６の発明によれば、利用者の本人確認を行った後、利用者固有の暗号鍵情報を送信するようにしているので、本人以外の第三者が端末保存データを利用者固有の暗号鍵情報を用いて不正に暗号化したり復号化したりするのを回避することができるという優れた効果がある。

【００８０】特に、請求項１２の発明によれば、情報通信端末に予め利用者固有の暗号鍵情報が保存されていない場合でも、必要に応じて利用者固有の暗号鍵情報を通信回線を介して取得し、端末保存データの暗号化や復号化に用いることができることができるという優れた効果がある。

【００８１】特に、請求項１３の発明によれば、暗号鍵管理用情報処理装置で利用者の本人確認を行った後、利用者固有の暗号鍵情報を情報通信端末に送信することができるので、本人以外の第三者が端末保存データを利用者固有の暗号鍵情報を用いて不正に暗号化したり復号化したりするのを回避することができるという優れた効果がある。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図。

【図２】同端末保存データ移動方法に用いられるユーザ管理サーバの概略構成図。

【図３】同ユーザ管理サーバの機能ブロック図。

【図４】同端末保存データ移動方法に用いられる携帯電話機の概略構成図。

【図５】同携帯電話機の機能ブロック図。

【図６】同端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャート。

【図７】変形例に係るデータ移動手順の流れを示すフローチャート。

【図８】本発明の第２の実施形態に係る端末保存データ移動方法の全体の枠組みを示す概念図。

【図９】同端末保存データ移動方法に用いられるユーザ管理サーバの機能ブロック図。

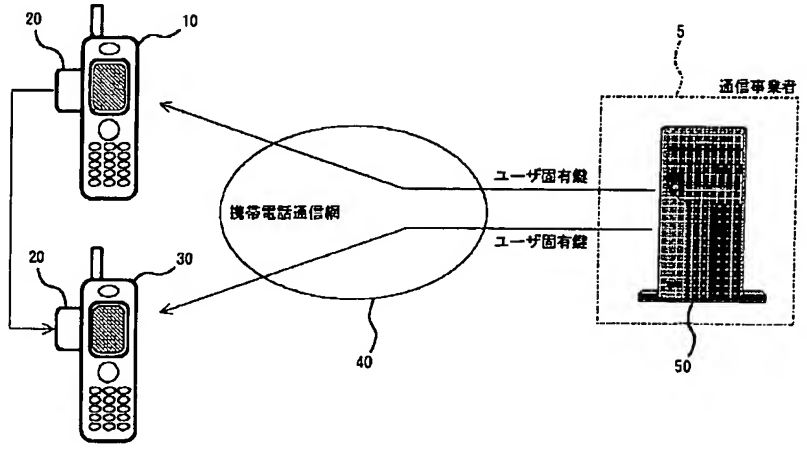
【図１０】同端末保存データ移動方法に用いられる携帯電話機の機能ブロック図。

【図１１】同端末保存データ移動方法におけるデータ移動手順の流れを示すフローチャート。

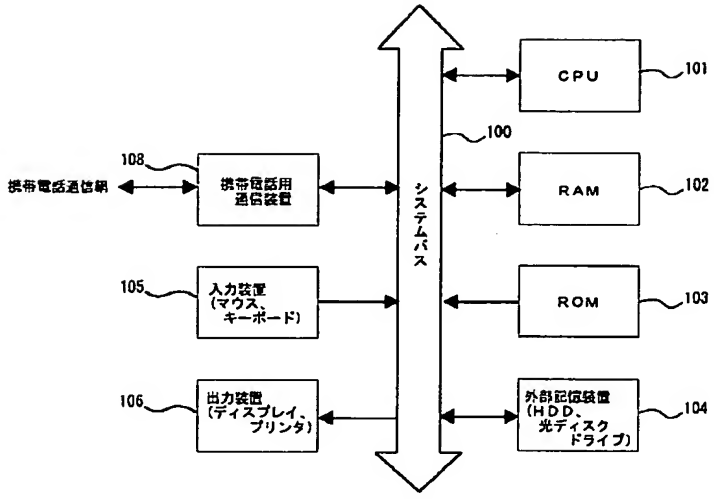
【符号の説明】

１０　交換前の携帯電話機
２０　メモリーカード
３０　交換後の携帯電話機
４０　携帯電話通信網
５０　ユーザ管理サーバ
１００　システムバス
１０１　ＣＰＵ
１０２　ＲＡＭ
１０３　ＲＯＭ
１０４　外部記憶装置
１０５　入力装置
１０６　出力装置
１０８　携帯電話用通信装置
２００　システムバス
２０１　ＣＰＵ
２０２　ＲＡＭ
２０３　ＲＯＭ
２０４　入力装置
２０５　出力装置
２０６　メモリーカードドライブ装置
２０７　携帯電話用通信装置
５０１　利用者情報記憶手段
５０２　暗号鍵情報生成手段
５０３　暗号鍵情報送信手段
５０４　端末保存データ受信手段
５０５　端末保存データ記憶手段
５０６　端末保存データ送信手段
６０１　端末保存データ記憶手段
６０２　暗号鍵情報受信手段
６０３　暗号鍵情報記憶手段
６０４　暗号化手段
６０５　データ書込手段
６０６　データ読込手段
６０７　復号化手段
６０８　端末保存データ送信手段
６０９　端末保存データ受信手段

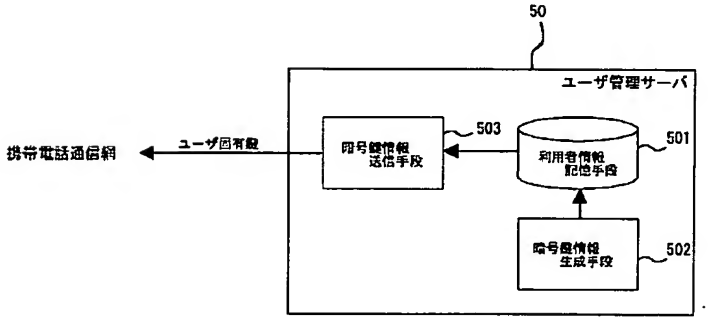
【図１】



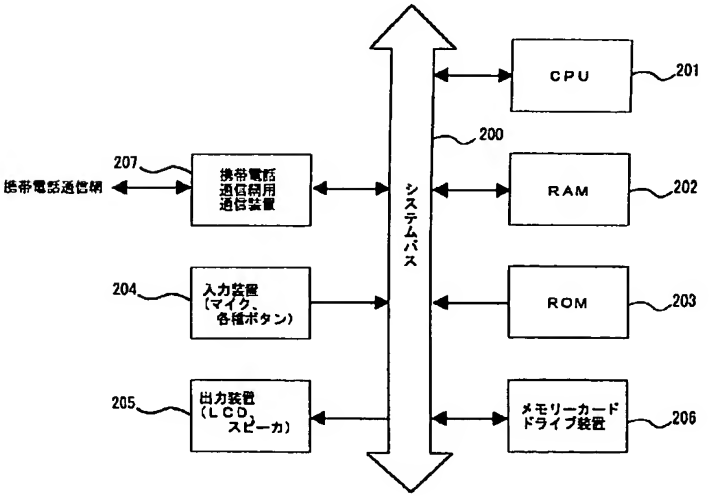
【図２】


CPU
101
100
RAM
102
ROM
103
外部記憶装置
(HDD、
光ディスク
ドライブ)
104
システムバス
108
携帯電話用
通信装置
携帯電話通信網
105
入力装置
(マウス、
キーボード)
106
出力装置
(ディスプレイ、
プリンタ)

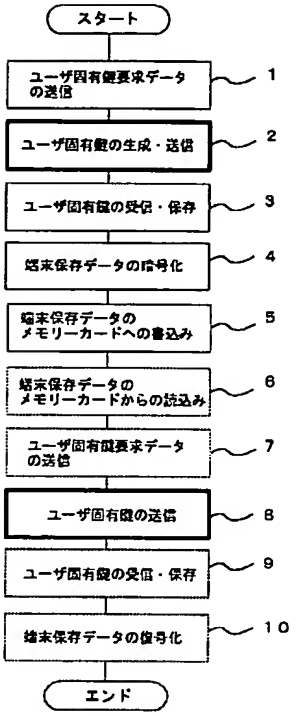
【図３】


50
ユーザ管理サーバ
携帯電話通信網
ユーザ固有鍵
暗号鍵情報
送信手段
503
利用者情報
記憶手段
501
暗号鍵情報
生成手段
502

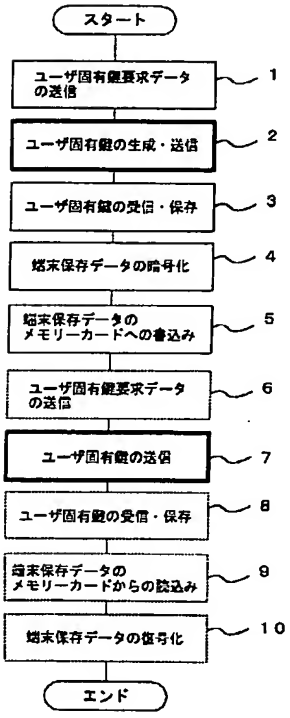
【図４】


CPU
201
200
RAM
202
ROM
203
メモリーカード
ドライブ装置
206
システムバス
207
携帯電話
通信網用
通信装置
携帯電話通信網
204
入力装置
(マイク、
各種ボタン)
205
出力装置
(LCD、
スピーカ)

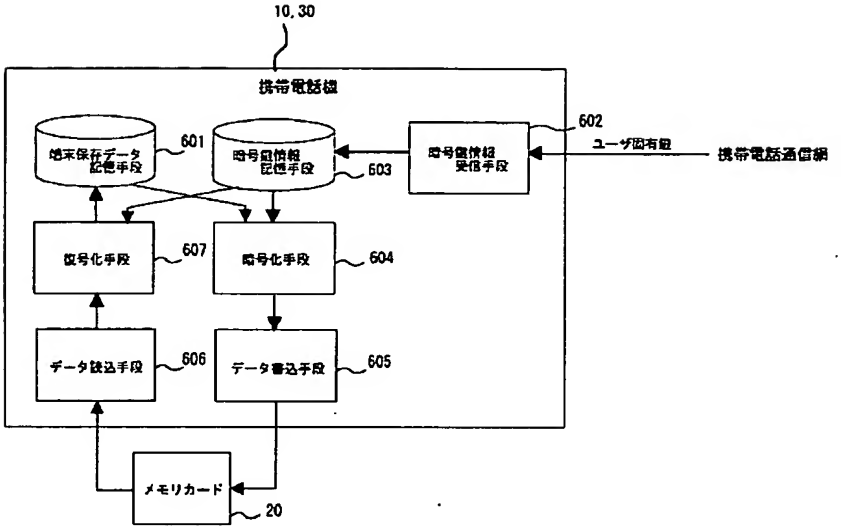
【図６】


スタート
ユーザ固有鍵要求データ
の送信
1
ユーザ固有鍵の生成・送信
2
ユーザ固有鍵の受信・保存
3
端末保存データの暗号化
4
端末保存データの
メモリーカードへの書込み
5
端末保存データの
メモリーカードからの読込み
6
ユーザ固有鍵要求データ
の送信
7
ユーザ固有鍵の送信
8
ユーザ固有鍵の受信・保存
9
端末保存データの復号化
10
エンド

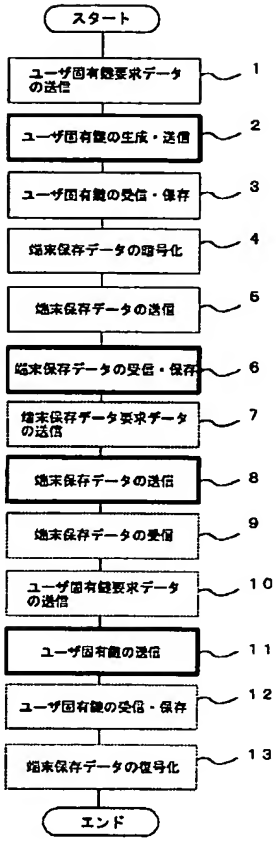
【図７】


スタート
ユーザ固有鍵要求データ
の送信
1
ユーザ固有鍵の生成・送信
2
ユーザ固有鍵の受信・保存
3
端末保存データの暗号化
4
端末保存データの
メモリーカードへの書込み
5
ユーザ固有鍵要求データ
の送信
6
ユーザ固有鍵の送信
7
ユーザ固有鍵の受信・保存
8
端末保存データの
メモリーカードからの読込み
9
端末保存データの復号化
10
エンド

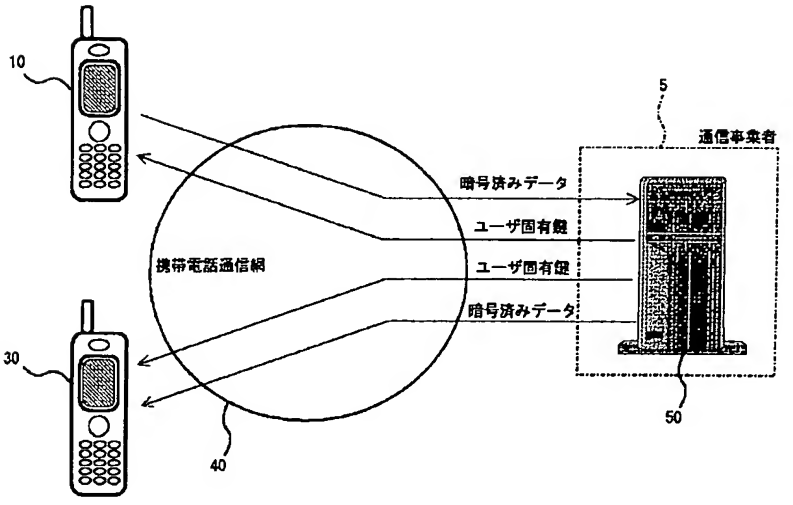
【図５】


10, 30
携帯電話機
端末保存データ記憶手段
601
暗号鍵情報記憶手段
603
暗号鍵情報受信手段
602
ユーザ固有鍵
携帯電話通信網
復号化手段
607
暗号化手段
604
データ読込手段
606
データ書込手段
605
メモリカード
20

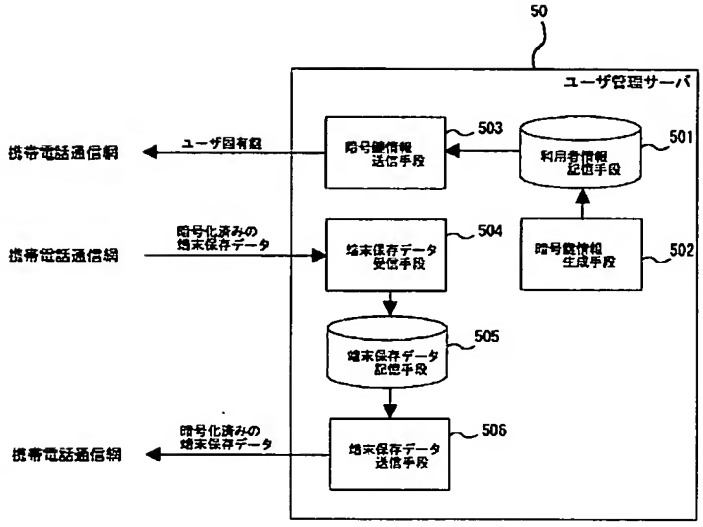
【図１１】


スタート
ユーザ固有鍵要求データの送信
1
ユーザ固有鍵の生成・送信
2
ユーザ固有鍵の受信・保存
3
端末保存データの暗号化
4
端末保存データの送信
5
端末保存データの受信・保存
6
端末保存データ要求データの送信
7
端末保存データの送信
8
端末保存データの受信
9
ユーザ固有鍵要求データの送信
10
ユーザ固有鍵の送信
11
ユーザ固有鍵の受信・保存
12
端末保存データの復号化
13
エンド

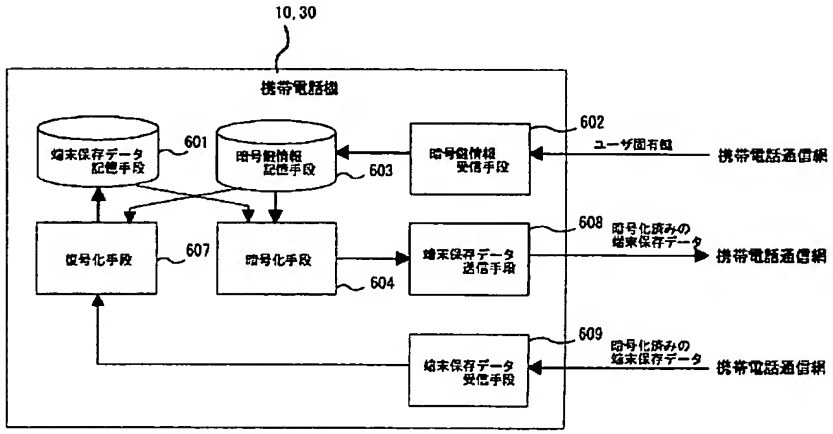
【図８】


10
30
携帯電話通信網
40
5
通信事業者
暗号済みデータ
ユーザ固有鍵
ユーザ固有鍵
暗号済みデータ
50

【図９】



【図１０】



フロントページの続き

(51) Int. Cl.[7] 識別記号 F I テーマコード(参考)
H04L 9/32 H04L 9/00 621A

(72)発明者 深谷 真人
東京都新宿区信濃町34番地 ＪＲ信濃町ビル ジェイフォン東日本株式会社内

Fターム(参考) 5B017 AA03 BA07 CA15 CA16
5B082 GA11 HA05
5J104 AA16 EA04 EA26 NA02 NA27
PA02 PA14